IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JONETHAN JAMES, on behalf of himself and all others similarly situated, Plaintiff, v. **NEXTGEN HEALTHCARE, INC.** Defendant.	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jonethan James ("Plaintiff") brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class Members"), against NextGen Healthcare, Inc. ("Defendant" or "NextGen") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach where unauthorized third-party criminals accessed and exfiltrated personal

data NextGen's network that resulted in unauthorized access to the highly sensitive consumer data[1] of Plaintiff and at least 1,049,375 Class Members ("Data Breach").[2]

2. NextGen is a leading provider of cloud-based healthcare technology solutions. NextGen develops and sells electronic health record ("EHR") software and practice management systems to customers in the healthcare industry, including medical, behavioral, and oral health providers.

3. Information compromised in the Data Breach includes personally identifying information ("PII") and protected health information ("PHI") such as names, addresses, dates of birth, and Social Security numbers (collectively, "PII" and "PHI" is "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that Defendant collected and maintained.

5. Defendant maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on

[1] NextGen Healthcare, Inc's Sample Breach Notice (Apr. 28, 2023), https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8/6102f57f-d60d-4b59-aa4d-7c30e68a2f68/document.html (the "Notice Letter").

[2] Office of the Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last visited May 10, 2023).

Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a vulnerable condition. In addition, NextGen and its employees failed to properly monitor the computer network and IT systems that housed the Private Information.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiff and Class

Members have and will continue to suffer injuries associated with this risk, including but not limited to as a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

8. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

9. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence; (ii) breach of implied contract; (iii) unjust enrichment; and (iv) breach of fiduciary duty. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

THE PARTIES

Plaintiff Jonethan James

10. Plaintiff Jonethan James is a natural person, resident, and a citizen of the State of Michigan. Mr. James has no intention of moving to a different state in the immediate future. Plaintiff James is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff James's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff James's Private Information was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

11. Plaintiff received a notice letter from Defendant dated April 28, 2023, stating that an unknown actor accessed and obtained certain files on the NextGen's network containing Private Information between March 29, 2023 and April 14, 2023.

Defendant NextGen Healthcare, Inc.

12. Defendant NextGen Healthcare, Inc. is a Georgia corporation with its principal place of business at 3525 Piedmont Road NE, Building 6, Suite 700, Atlanta, Georgia 30305. Defendant is a citizen of the State of Georgia.

JURISDICTION AND VENUE

13. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including Plaintiff James, are citizens of a different state than Defendant NextGen, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

14. This Court has general personal jurisdiction over Defendant NextGen because NextGen maintains its principal place of business in Atlanta, Georgia regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because NextGen's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANT'S BUSINESS

16. NextGen is a software & services company that develops and sells electronic health record software and practice management systems to the healthcare industry. NextGen maintains seven offices, has over 2,800 employees and generates approximately $625.9 million in yearly revenue. NextGen trades on Nasdaq stock exchange under the stock symbol NXGN.

17. NextGen offers electronic health records (EHR), electronic data interchange (EDI), practice management, revenue cycle management, patient engagement, telehealth, billing, and other solutions to healthcare industry clients.

18. In its "Notice of Data Security Incident" sent to several State Attorneys General, NextGen acknowledges that it collects and stores Private Information of its customers' patients, including Plaintiff and the Class. "In support of the services we provide to your medical professionals, we maintain certain of your personal information on their behalf."[3]

19. Defendant's Privacy Policy, posted on its website, acknowledges that, as part of its business, involves "access to, and the processing of, patient information…such information may be considered Protected Health Information as the term is defined in the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("HIPPA").

20. Defendant claims that, "We take very seriously the security and privacy of your information, and deeply regret any inconvenience this may cause."[4]

21. To obtain healthcare related services, patients, like Plaintiff and Class Members, must provide their doctors or medical professionals or Defendant directly with highly sensitive Private Information. As part of its business, Defendant then

[3] *See* Notice Letter.
[4] See *id.*

compiles, stores, and maintains the Private Information it receives from the healthcare professionals who utilize Defendant's services. Defendant has served thousands of individuals since its founding in 1974, indicating that that it has created and maintains a massive repository of Private Information, acting as particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

22. On information and belief, in the ordinary course of its business of providing medical care and services, NextGen maintains the Private Information of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;
- Health insurance information;

- Photo identification;
- Employment information, and;
- Other information that Defendant may deem necessary to provide care.

23. Additionally, Defendant may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family members.

24. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to patients and other individuals, NextGen, upon information and belief, promises to, among other things: keep protected health information private; comply with health care industry standards related to data security and Private Information, including HIPAA; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

25. As a HIPAA covered business entity (*see infra*), NextGen is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA

Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

26. However, NextGen did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly six months to disclose the Data Breach publicly.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

NextGen is a Business Associate Subject to HIPAA

28. NextGen is an HER vendor subject to HIPAA covered entity that provides services to healthcare and medical service providers. As a regular and necessary part of its business, NextGen collects and custodies the highly sensitive Private Information of its clients' patients. NextGen's clients are Covered Entities under HIPAA. As a business associate who is regularly engaged by HIPAA Covered Entities, NextGen is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it acquires, receives, and

collects, and NextGen is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

29. Under HIPAA, a business associate is a person or entity who creates, receives, maintains or transmits PHI on behalf of (or for the benefit of) a covered entity (directly or through another business associate) to carry out covered functions of the covered entity.[5]

30. As a business associate of HIPAA covered entities, NextGen is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

31. Due to the nature of NextGen's business, which includes providing a range of medical technology services, including storing and maintaining electronic health records, NextGen would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

[5] https://www.hhs.gov/guidance/document/faq-3013-does-hipaa-require-covered-entity-or-its-ehr-system-developer-enter-business (last visited May 7, 2023).

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, NextGen assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

33. Plaintiff and Class Members are or were patients whose medical records and Private Information were maintained by, or who received health-related or other services from, NextGen and directly or indirectly entrusted NextGen with their Private Information.

34. Plaintiff and the Class Members relied on NextGen to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiff and Class Members reasonably expected that NextGen would safeguard their highly sensitive information and keep their Private Information confidential.

35. As described throughout this Complaint, NextGen did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect

the highly sensitive information NextGen maintained. Consequently, cybercriminals circumvented NextGen's security measures, resulting in a significant data breach.

THE DATA BREACH AND NOTICE LETTER

36. According to the Notice Letter NextGen provided to Plaintiff and Class Members, as well as to State Attorneys General, NextGen was subject to a cybersecurity attack where unauthorized parties accessed Private Information on NextGen's networks between March 29, 2023 and April 14, 2023.[6]

37. On March 30, 2023, NextGen was alerted to unusual activity on its network. In response, Defendant worked with "third-party forensic experts" to conduct an investigation and "too measures to contain the incident."[7]

38. Through its investigation, NextGen determined that "an unknown third-party gained unauthorized access unauthorized actor accessed certain files and data stored within our systems."[8]

39. According to the Notice Letter, the affected information included individuals' "name, date of birth, address and Social Security number."[9]

40. "As soon as we discovered the suspicious activity…we took measures to contain the incident, including resetting passwords, and further reinforcing the

[6] *See* Notice Letter.
[7] See *id.*
[8] *See id.*
[9] *See id.*

security of our system."[10] Defendant admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' Private Information going forward.

41. In the Notice Letter Defendant recommended that Plaintiff and Class Members "remain vigilant by reviewing account statements and credit reports closely."[11] However, the letter also acknowledged that Plaintiff and Class Members may only "obtain a free copy of [their] credit report from each of the three major credit reporting agencies once every 12 months."[12]

42. The Notice Letters further provided the following "Additional Steps to Help Protect Your Information":

> **Report Suspicious Activity or Suspected Identity Theft.** If you detect any unauthorized or suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. If you suspect any identity theft has occurred, you can contact your local law enforcement by filing a police report or the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338), by writing to the FTC at 600 Pennsylvania Avenue, NW Washington DC 20580, or online at www.ftc.gov. You can also contact your state Attorney General
>
> …

[10] *See id.*
[11] See https://apps.web.maine.gov/online/aeviewer/ME/40/ad13358b-45d7-4d7a-96a3-e6e56e2c10b2/b6e49831-4833-4d8f-9484-43617557c119/document.html (last visited Apr. 6, 2023).
[12] *Id.*

Contacting the Internal Revenue Service: If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, you should immediately contact the IRS or state tax agency as appropriate. For the IRS, you can use Form 14039 (https://www.irs.gov/pub/irs-pdf/f14039.pdf). You can also call them at 800-908-4490 (Identity Theft Hotline). Information on how to contact your state department of revenue to make similar reporting may be found by going to http://www.taxadmin.org/state-tax-agencies.

…

Fraud Alert: As a precautionary step, to protect yourself from possible identity theft you can place a fraud alert on your bank accounts and credit file. A fraud alert tells creditors to follow certain procedures before opening a new account in your name or changing your existing account. You may call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. All three credit reports will be sent to you, free of charge, for your review.

…

Security Freeze: In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. There may be a fee for this service based on state law (in MA, there shall be no charge). To put a security freeze on your credit file contact the consumer reporting agencies listed below [13]

[13] *See, e.g., id.*

43. Upon information and belief, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

44. Upon information and belief, the accessed systems contained Private Information and that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

45. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which NextGen was aware and knew it had a duty to guard against. This is particularly true because the targeted attack was a ransomware attack. It is well-known that healthcare businesses such as Defendant, which collect and store the confidential and sensitive PII/PHI of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

46. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

47. Defendant had obligations created by HIPAA, the FTC Act, contract, industry standards, common law, and its own promises and representations made to

Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

48. Plaintiff and Class Members provided their Private Information to NextGen with the reasonable expectation and mutual understanding that NextGen would comply with its obligations to keep such information confidential and secure from unauthorized access.

49. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, NextGen assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

50. Due to NextGen's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

51. As a business associate to healthcare providers, Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

52. At all relevant times, NextGen knew, or should have known that Plaintiff's, and Class Members' Private Information was a target for malicious actors. Despite such knowledge, NextGen failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that NextGen should have anticipated and guarded against.

53. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

54. In light of recent high profile data breaches at other health care providers, Defendant knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

55. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

[14] *2022 Breach Barometer*, PROTENUS, *see* https://blog.protenus.com/key-takeaways-from- the-2022-breach-barometer (last visited May. 7, 2023).

56. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[15]

57. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

58. Indeed, cyberattacks against the healthcare industry have been common for over eleven years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is

[15] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector- suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited May. 7, 2023).

compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[16]

59. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[17] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[18] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[19]

60. Cyberattacks on medical systems like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential

---

[16] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited May 7, 2023).

[17] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited May. 7, 2023).

[18] *Id.*

[19] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited May 7, 2023).

targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[20]

61. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [21]

62. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[22]

---

[20] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited May 7, 2023).
[21] https://www.hipaajournal.com/why-do-criminals-target-medical-records(last visited May. 7, 2023).
[22] See *id.*

63. Private Information, like that stolen from NextGen, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[23]

64. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

65. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[24]

66. NextGen was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the

[23] See *id*.
[24] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack*(last visited May. 7, 2023).

purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[25]

67. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[26]

68. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

69. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies

---

[25] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited May 7, 2023).

[26] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited May 7, 2023).

approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[27]

70. As a HIPAA covered business associate, NextGen should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

Defendant Fails to Comply with FTC Guidelines

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no

[27] https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops (last visited May 7. 2023).

longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[28] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[29]

73. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the

[28] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 7, 2023).
[29] *Id*.

Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

76. Defendant failed to properly implement basic data security practices.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Defendant was at all times fully aware of its obligation to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

79. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks

because of the value of the Private Information which they collect and maintain.

80. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

81. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

82. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity

readiness.

83. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Defendant's Violated HIPAA Obligations to Safeguard Private Information

84. By offering Electronic Health Records and Practice Management software and services, as well as other services to the healthcare industry, NextGen is a covered business associate under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

85. HIPAA requires covered business associates to protect against reasonably anticipated threats to the security of sensitive patient health information.

86. NextGen is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

87. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

88. HIPAA covered business associates must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

89. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

90. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

91. The Data Breach resulted from a combination of insufficiencies that demonstrate NextGen failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

92. Cyberattacks and data breaches at healthcare companies and associated companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

93. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[30]

94. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[31]

95. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of

[30] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited May 7, 2023).
[31] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

identity theft face "substantial costs and time to repair the damage to their good name and credit record."[32]

96. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

---

[32] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited May 7, 2023).

97. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[33]

98. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

99. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[33] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 7, 2023).

100. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[34]

101. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

102. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

103. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> *See* GAO Report, at p. 29.

[34] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

104. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

105. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

106. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

107. Private Information can sell for as much as $363 per record according to the Infosec Institute.[35] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

108. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[36] Such fraud may go undetected until debt collection calls

[35] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 7, 2023).

[36] *Identity Theft and Your Social Security Number*, Social Security Administration

commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[37] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

109. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

110. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

111. This data, as one would expect, demands a much higher price on the

(2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 7, 2023).

[37] *Id*.

[38] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 7, 2023).

black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[39]

112. Medical information is especially valuable to identity thieves.

113. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[40]

114. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

---

[39] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited May 7, 2023).

[40] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Apr. 6, 2023).

115. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

116. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet NextGen failed to properly prepare for that risk.

DEFENDANT'S DATA BREACH

117. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access

reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA

Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

118. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access NextGen's computer network and systems for 16 days which contained unsecured and unencrypted Private Information.

119. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Plaintiff's and Class Members' Damages

120. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Yet, to date, Defendant has merely offered to provide victims of the Data Breach with limited subscriptions to fraud and identity monitoring services. This does nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Nor will it prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach. And at the conclusion of these limited subscriptions, victims will be required to pay for such services out of their own pocket.

121. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

122. Plaintiff's and Class Members' names, dates of birth, addresses, and Social Security Numbers were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system(s).

123. Since being notified of the Data Breach, Plaintiff James has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

124. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

125. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

126. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

127. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

128. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

129. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private

Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

130. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

131. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

132. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant's healthcare customers was intended to be used by Defendant to fund adequate security of its computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

133. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

134. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

135. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

136. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

137. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff James's Experience

138. Plaintiff James never provided his Private Information to NextGen Healthcare directly, but upon information and belief, Mr. James obtained medical products and/or services at a medical facility that contracted with NextGen, at some point in recent years.

139. According to the Data Breach Notice Letter, dated April 28, 2023, that Defendant sent, via U.S. mail, to Plaintiff James, NextGen Healthcare acquired and maintained Plaintiff James's Private Information from one of Plaintiff James's doctors and/or medical professionals.

140. Upon information and belief, Plaintiff was presented with standard forms to complete prior to receiving medical services that required his PII and PHI. Upon information and belief, Defendant received and maintains the information Plaintiff James was required to provide to his doctors or medical professionals. Plaintiff also believes he was presented with standard HIPAA privacy notices before disclosing his Private Information to his medical provider(s).

141. Plaintiff James is very careful with his Private Information. He stores any documents containing Private Information in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

142. As a result of the Data Breach, Plaintiff James made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to, researching the Data Breach, checking his credit scores regularly, and reviewing credit card and financial account statements for any indication of fraudulent activity, which may take years to detect.

143. Plaintiff James was forced to spend significant time attempting to mitigate the effects of the Data Breach and safeguard himself from its consequences. He will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

144. Plaintiff James suffered actual injury and damages from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of intangible property that NextGen Healthcare obtained from Plaintiff James's doctors and medical professionals; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time; (e) loss of benefit of the bargain; and

(f) imminent and impending injury arising from the increased risk of identity theft and fraud.

145. Plaintiff James has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud.

146. As a result of the Data Breach, Plaintiff James anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff James will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

147. Plaintiff James has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

148. Plaintiff brings this action against NextGen on behalf of himself and on behalf of all other persons similarly situated ("the Class").

149. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All persons NextGen identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

150. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

151. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses as this case progresses.

152. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Defendant disclosed to the Maine Attorney General that the Private Information of approximately 1,049,375 Class Members was compromised in Data Breach.

153. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

154. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

155. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

156. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

157. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

158. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

159. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

160. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

161. Plaintiff re-alleges and incorporates by reference paragraphs 1-160 as if fully set forth herein.

162. By collecting and storing the Private Information of Plaintiff and Class Members, this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a

reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

163. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

164. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

165. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

166. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health

information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

167. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

168. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

169. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

170. Plaintiff and Class Members had no ability to protect their Private Information that was or remains in Defendant's possession.

171. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

172. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

173. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

174. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

175. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

176. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's

breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

177. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

178. Plaintiff re-alleges and incorporates by reference paragraphs 1-160 as if fully set forth herein.

179. Defendant acquired and maintained the Private Information of Plaintiff and the Class that it received either directly or from its healthcare provider customers.

180. When Plaintiff and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals and their business associates, including Defendant.

181. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information

and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

182. Plaintiff and the Class were required to deliver their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

183. Defendant NextGen solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

184. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

185. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

186. In delivering their Private Information to Defendant and providing paying for healthcare services, Plaintiff and Class Members intended and

understood that Defendant would adequately safeguard the data as part of that service.

187. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

188. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

189. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

190. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Private Information to Defendant.

191. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

192. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

193. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

194. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

195. Plaintiff re-alleges and incorporates by reference paragraphs 1-160 as if fully set forth herein.

196. This count is pleaded in the alternative to breach of implied contract claim above (Count II).

197. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

198. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

199. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and/or services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

200. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

201. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of NextGen's rendering of services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Private Information, and by providing Defendant with their valuable Private Information.

202. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

203. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members,

because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

204. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

205. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

206. Plaintiff and Class Members have no adequate remedy at law.

207. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

208. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

209. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
Breach Of Fiduciary Duty
(On Behalf Of Plaintiff And The Class)

210. Plaintiff re-alleges and incorporates by reference paragraphs 1-160 as if fully set forth herein.

211. In light of the special relationship between Defendant and Plaintiff and Class Members, Defendant became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant does store.

212. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their Private Information.

213. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

214. Defendant breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

215. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

216. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, pursuant to O.C.G.A. § 13-6-11, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury of any and all issues in this action so triable as of right.

Dated: May 11, 2023

Respectfully Submitted,

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Tel.: 404-320-9979
Fax: 404-320-9978
mgibson@thefinleyfirm.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiff

** Pro Have Vice Forthcoming*

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14-point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: May 11, 2023.

/s/ MaryBeth V. Gibson
MARYBETH V. GIBSON